CLAIMS:

What is claimed is:

1. A method in a digital camera for verifying that a particular digital visual image was produced by said digital camera, said method comprising the steps of:

storing a visual image in a digital format in said camera;

generating a digital signature for said image utilizing said camera only in response to said storage of said image in said camera, said digital signature associating said stored image with said camera;

storing said digital signature only in said camera, said signature being stored separately from said image in said camera, said digital signature capable of being utilized only within said camera by only said camera, wherein said signature is inaccessible to devices other than said camera; and

subsequently authenticating said particular digital visual image as being produced by said digital camera utilizing said digital signature stored in said digital camera, wherein only said digital camera is capable of authenticating said particular digital visual image.

2. The method according to claim 1, further comprising the steps of:

storing said visual image in a file within said camera, said file being designated by a filename; and

storing said signature in said camera with said filename.

3. The method according to claim 1, further comprising the steps of:

establishing a hardware master key pair for said digital camera, said hardware master key pair including a master private key and a master public key, said hardware master key pair being associated with said digital camera so that said master private key is known to only said digital camera;

establishing a signature device having an encryption engine and a protected storage device, said protected storage device being accessible only through said encryption engine; and

storing said hardware master key pair in said protected storage device.

4. The method according to claim 3, wherein said step of generating a digital signature further comprises the steps of:

hashing said stored image to produce an original image digest;

signing said first digest utilizing said master private key; and

storing said signed original image digest as said signature.

5. The method according to claim 4, wherein said step of authenticating said visual image further comprises the steps of:

retrieving an image to authenticate;

retrieving a signature for said image which is to be authenticated;

hashing said image which is to be authenticated to produce a first digest;

decrypting said retrieved signature to retrieve a second digest;

comparing said first digest to said second digest;

determining that said image has been altered in response to a determination that said first and second digests do not match; and

determining that said image has not been altered in response to a determination that said first and second digests match.

6. The method according to claim 1, wherein said step of generating a digital signature further comprises the steps of:

hashing said stored image to produce an original image digest;

signing said first digest utilizing a master private key; and

storing said signed original image digest as said signature.

7. The method according to claim 6, wherein said step of authenticating said visual image further comprises the steps of:

retrieving an image to authenticate;

retrieving a signature for said image which is to be authenticated;

hashing said image which is to be authenticated to produce a first digest;

decrypting said retrieved signature to retrieve a second digest;

comparing said first digest to said second digest;

determining that said image has been altered in response to a determination that said first and second digests do not match; and

determining that said image has not been altered in response to a determination that said first and second digests match.

8. A digital camera for verifying that a particular digital visual image was produced by said digital camera, comprising:

memory means for storing a visual image in a digital format in said camera;

a signature device for generating a digital signature for said image utilizing said camera only in response to said storage of said image in said camera, said digital signature associating said stored image with said camera;

memory means for storing said digital signature only in said camera, said signature being stored separately from said image in said camera, said digital signature capable of being utilized only within said camera by only said camera, wherein said signature is inaccessible to devices other than said camera; and

means for subsequently authenticating said particular digital visual image as being produced by said digital camera utilizing said digital signature stored in said digital camera, wherein only said digital camera is capable of authenticating said particular digital visual image.

9. The digital camera according to claim 8, further comprising:

said memory means for storing said visual image in a file within said camera, said file being designated by a filename; and

said memory means for storing said signature in said camera with said filename.

10. The digital camera according to claim 8, further comprising:

said signature device including stored within it a hardware master key pair for said digital camera, said hardware master key pair including a master private key and a master public key, said hardware master key pair being associated with said digital camera so that said master private key is known to only said digital camera; and

said signature device having an encryption engine and a protected storage device, said protected storage device being accessible only through said encryption engine.

11. The digital camera according to claim 10, further comprising:

means for hashing said stored image to produce an original image digest;

means for signing said first digest utilizing said master private key; and

means for storing said signed original image digest as said signature.

12. The digital camera according to claim 11, further comprising:

means for retrieving an image to authenticate;

means for retrieving a signature for said image which is to be authenticated;

means for hashing said image which is to be authenticated to produce a first digest;

means for decrypting said retrieved signature to retrieve a second digest;

means for comparing said first digest to said second digest;

means for determining that said image has been altered in response to a determination that said first and second digests do not match; and

means for determining that said image has not been altered in response to a determination that said first and second digests match.

13. The digital camera according to claim 8, further comprising:

means for hashing said stored image to produce an original image digest;

means for signing said first digest utilizing a master private key; and

means for storing said signed original image digest as said signature.

14. The digital camera according to claim 13, further comprising:

means for retrieving an image to authenticate;

means for retrieving a signature for said image which is to be authenticated;

means for hashing said image which is to be authenticated to produce a first digest;

means for decrypting said retrieved signature to retrieve a second digest;

means for comparing said first digest to said second digest;

means for determining that said image has been altered in response to a determination that said first and second digests do not match; and

means for determining that said image has not been altered in response to a determination that said first and second digests match.